EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCC SCHEME

GUIDANCE

AUTHORISATION OF CBs AND ITSEFs FOR THE EUCC SCHEME

Version 0.7, June 2024

DOCUMENT HISTORY

Date of change	Version	Modification	Clarification
December 2023	0.0	First outlines of the document	Creation of the State-of-the-Art document
January 2024	0.1	First raw draft of some paragraphs and content elements proposed	Outlines of paragraphs and first introduction of content proposed for discussion & comments
January 22nd 2024	0.2	Comments processed of CCN, BSI & FME	Corrections, clarifications and text rewriting based upon the comments provided by the group and discussion outcomes.
February 1st 2024	0.3	Fill the paragraphs of planning with amongst others re-use some content of early guidance documentation based upon EU CC version 1.1.1. and share for review by group	Corrections, clarifications and text rewriting based upon the comments provided by the group and discussion outcomes.
February 18th	0.4	Process input and comments of the group and added new text for the open items. Fill the paragraphs of planning with amongst others re-use some content of early guidance documentation based upon EU CC version 1.1.1. and share for review by group	Corrections, clarifications and text rewriting based upon the comments provided by the group and discussion outcomes.
February 19th	0.4.1. 0.4.2.	Upon the SoA review of Accreditation some minor amendments are made in the text to ensure alignment Minor updates in green text were added when making the presentation for the group	Some amendments of minor importance were made
March 20-26	0.5	Processing of comments of NABs and MSs based upon the shared version 0.4.1. with EA and ECCG and rearranging the text, take out the preparation procedure	Simplify the document and improve readability
April 4 2024	0.5.1	Corrections based on EC comments	Version to be submitted to ECCG comments
10 June 2024	0.6	Transformation of the document into guidance Corrections based on ECCG comments	Version to be submitted to ECCG endorsement
25 June 2024	0.7	Correction of the text to distinguish between existing legally binding rules and guidance	Approved for publication on 16/07/2024 by the ECCG and the European Commission

LEGAL INFORMATION

LEGAL NOTICE

This publication is established in accordance with recital 18 of Commission Implementing Regulation (EU) 2024/482**.**

This document is a guidance document established and endorsed by the European Cybersecurity Certification Group (ECCG) in accordance with Article 48 (2-3) of Commission Implementing Regulation (EU) 2024/482.

The document shall be updated where developments and best practices in the field of authorisation require to do so. Updates of this document shall be submitted to the ECCG.

This document shall be read in conjunction with Regulation (EU) 2019/881, the Commission Implementing Regulation (EU) 2024/482, its annexes and where applicable supporting documentation that is made available.

This guidance document is made publicly accessible through the EU cybersecurity certification website and is free of charge.

ENISA is not responsible or liable for the use of the content of this document. Neither ENISA nor any person acting on its behalf or on behalf for the maintenance of the scheme is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

CONTACT

Constructive feedback or questions related to this document are welcome, please use Cybersecurity Certification (europa.eu)

TABLE OF CONTENTS

1 INTRODUCTION

1. This guidance document [initially established as a state-of-the-art document as explained under recital 18 of Commission Implementing Regulation (EU) 2024/482 (hereinafter referred to as EUCC), and transformed into guidance upon request of the ECCG] is a supporting document for the authorisation of certification bodies (CBs) and Information Technology Security Evaluation Facilities (ITSEFs). The Regulation (EU) 2019/881 (hereinafter referred to as the EU Cybersecurity Act - CSA), foresees under Article 60 (3) of that Regulation the possibility that a cybersecurity certification scheme may include additional or specific requirements that a conformity assessment body (CAB) needs to meet to guarantee its technical competence to evaluate the cybersecurity requirements of that specific scheme, as defined under Article 54 (1) (f) CSA. It is the national cybersecurity certification authority (NCCA, the monitoring and supervising body) that is tasked to perform this assessment, which positive results will result in the 'authorisation' of the CAB.

2. Authorisation under EUCC therefore serves the specific purpose is to allow attesting that conformity assessment bodies have the technical competences for their conformity assessment activities where the ICT product or protection profile is to be certified under assurance level 'high' and have put in place appropriate technical and operational measures to effectively protect confidential and sensitive information for that assurance level.

3. EUCC provides under Article 21 the overview of the requirements related to the authorisation of Certification Bodies (CBs). The requirements for Information Technology Security Evaluation Facilities (ITSEFs) are defined under Article 22 EUCC. This guidance document serves to further provide common recommendations on the application, performance of, and compliance with authorisation requirements.

4. Why do these EUCC requirements apply for this assurance level 'high'? The ICT products [and protection profiles] need for that level to provide the assurance that they meet the cybersecurity requirements, including the security functionalities, and that they are evaluated at a level intended to minimise the risk of state-of-the-art-attacks carried out by actors with significant skills and resources, including state actors, APT hacking groups and hybrid forms of criminal and state actor attackers. Conformity assessment bodies in charge of such activities are therefore subject to national oversight and regular assessment by the monitoring and supervising NCCA to ensure that they meet the required capabilities, the technical skills, knowledge and practical expertise in the applicable domains.

2 ACRONYMS AND DEFINITIONS

APT	Advanced persistent threat
CAB	Conformity Assessment Body (Article 2 point 18 CSA)
CB	Certification Body (Article 2 point 12 EUCC)
CC	Common Criteria for Information Technology Security Evaluation.
CEM	Common Methodology for Information Technology Security Evaluation
EUCC	Commission Implementing Regulation (EU) 2024/482
CSA	Regulation (EU) 2019/881- Cybersecurity Act

EAL	Evaluation Assurance Level
EC	European Commission
ECCF	European Cybersecurity Certification Framework
ECCG	European Cybersecurity Certification Group (Article 62 CSA)
ENISA	European Union Agency for Cybersecurity
ETR	Evaluation Technical Report (Article 2 point 6 EUCC)
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and communications technology
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NAB	National Accreditation Body as defined in point (11) of Article 2 of Regulation (EC) No 765/2008
NCCA	National Cybersecurity Certification Authority (Article 58 CSA, Article 2 point 11 EUCC)
NIS2	Directive (EU) 2022/2555.
SMEs	Small and Medium Enterprises
SoA document	State-of-the-art document
SOG-IS	Senior Officials Group Information Systems Security
ToE	Target of Evaluation (Article 2 point 3 EUCC)
TOMs	Technical and organizational measures

3 THE INTERPLAY BETWEEN ACCREDITATION & AUTHORISATION

5. The accreditation and authorisation procedures are closely related to each other. Accreditation forms the baseline for CB and ITSEFs that want to operate under the European Cybersecurity Certification Framework (ECCF). To be authorised, accreditation is required. This does not necessarily imply that authorisation should be started after finalization of the accreditation. Ideally for reasons of efficiency and effectiveness, the CB and/or the ITSEF may decide to start the application for the authorisation before the accreditation is finalized or decide jointly prepare and apply for the authorisation assessment and the accreditation assessment. The NCCA

should indicate the possibilities and the related requirements for the options it provides to the ITSEF and CB.

6. Where the NCCA provides the opportunity in collaboration with the NAB to jointly perform the accreditation and authorisation in a combined assessment, the NAB and the NCCA shall each remain responsible for their own assessment, but are able to allow the CB and/or the ITSEF to plan it in the same period. This way they are able to apply around the same time and get a better picture on when they may be able to start their activities under EUCC.

7. Where the CB and ITSEF intent to jointly obtain the authorisation, there will be an assessment for the ITSEF and the CB to be planned with the NCCA. This implies that in terms of priority in authorisation decision making, the ITSEF authorisation assessment should be finalized prior to the finalisation of the authorisation of the CB to ensure that the CB meets the authorisation requirement under Article 21 (1) (b) EUCC: *the CB needs to conduct its activities with an "authorised ITSEF"*.

8. In the preparatory phase of the application for authorisation, and to support the cooperation between the CB and the ITSEF in accordance with Article 21 (1) (b) EUCC, the ITSEF may send the necessary documentation to the CB it will be working with for initial or preparatory review. Where the prior approval model of Article 56 (6) CSA is used, the CB may perform an initial document review with involvement of the prior approving body where the prior approval model requires this involvement.

9. Where the CB or ITSEF applied for authorisation simultaneously or close after the start of their accreditation application, it should inform the NCCA the moment it becomes aware of any delay in the accreditation process. The NCCA may upon non-conformities identified by the NAB regarding the ongoing accreditation procedure decide to postpone, or put the authorisation procedure temporarily "on hold" if this already started until the non-conformities are resolved by the CAB and approved by the NAB. As the authorisation and accreditation have the same duration of validity[1] the renewal of accreditation and authorisation is likely to take place in the same timeframe.

10. Once the CB or ITSEF accredited and authorised, the NAB and the NCCA should collaborate closely with each other in situation of potential or alleged non-compliance of these entities. Where issues around authorisation requirements come to surface, this should be notified to the NCCA in accordance with chapter 9. Where these issues touch upon accreditation requirements, also the National Accreditation Body[2] should be notified, as the NCCA should support the NAB actively during investigations with use of its investigative powers as provided by Article 58 (8) CSA. The NAB does not monitor the day-to-day practice of the conformity assessment bodies as such and for this reason, the NCCA has this legal obligation under Article 58 (7) (c) CSA. In this respect, the accreditation and authorisation should be seen as a joint effort to ensure that the conformity assessment bodies are continuously supported to become and remain compliant with the regular and specified requirements. The support that the NCCA should provide is without prejudice to the impartiality and independence of the NAB in the decisions the NAB needs to take. Even while the accreditation and authorisation are likely to be performed in the same period (simultaneously or not), the NAB and the NCCA shall both remain for each of their procedure fully responsible for their own assessment and shallform their findings and judgement independently from each other.

[1] We refer to Article 21 (4) EUCC and Article 22 (5) EUCC.

[2] The NAB is the sole body appointed by a Member State in accordance with Article 4 under Regulation (EC) 765/2008 that performs accreditation with authority derived from the State.

11. If during the accreditation the NAB upon a confirmed non-compliance of one or more elements related to the accreditation requirements of the CB, the ITSEF or their subcontracted party, takes the measure to restrict[3], or suspend the accreditation, this is expected to have an impact on the status of authorisation. For this reason, the NAB should notify the NCCA of the start of the non-compliance procedure, the progress, a foreseen status change of the accreditation and its outcome. The NCCA should actively support the NAB in this respect.

12. This requires a frequent exchange of information necessary[4] to address the matters related to actual cases, as well as in complaints handling cases which may serve as important input for the performance of a compliance audit performed by the NCCA[5]. In accordance with Article 58 (7) (g) CSA, the NCCA shall provide an annual summary report that amongst others includes the active assistance and support to the NAB and shall describe these activities as well as the use of the monitoring and supervising powers under Article 58 (8) CSA. This annual summary report shall be sent to the ECCG and ENISA.

13. More generic information like analysis in trends of non-compliance, types of complaints and other general information may be shared as well for the purpose of effective support in the tasks of the NAB and NCCA have. At the same time, this close interaction should support the task of the ECCG on:

    a. The *"examination of relevant developments in the field of cybersecurity certification and to exchange information and good practices on cybersecurity certification schemes"* (Article 62 (4)(f) CSA);
    b. The facilitation of "*the cooperation between national cybersecurity certification authorities under this Title through capacity-building and the exchange of information, in particular by establishing methods for the efficient exchange of information relating to issues concerning cybersecurity certification schemes"* (Article 62 (4)(g) CSA).

14. For the continuity of the cybersecurity certification market and its effectiveness it is of utmost importance that the CB and ITSEF and where applicable their subcontracted parties should be closely involved in non-compliance matters and given the opportunity to correct within a reasonable timeframe any alleged non-compliance related to authorisation requirements and as well as where accreditation is involved.

15. In this respect, decisions by the NAB and the NCCA related to withdrawal, restriction or suspension shall be carefully considered. Any change in status of the authorisation shall take all circumstances of the case into account. This implies that the decision shall be taken based upon the extent, nature, duration of the non-compliance and the impact of the non-compliance. The decision shall ensure that it is proportionate, non-discriminatory, justifiable and balanced. Particularly this is of importance where such an authorisation decision (or accreditation decision) has impact on the certification of ICT products or protection profiles in the process of certification, or impacts certifications which are used in the EU market, in critical infrastructure or in critical industry segments of the EU market, as this may significantly affect the entire EU market.

[3] Restriction of the authorisation corresponds to a reduction of its scope, as further detailed in Chapter 11.2.

[4] The sharing of information should take place in accordance with national and EU laws.

[5] See chapter 8 for the authorisation compliance audit.

3.1 THE TIMING OF THE START OF THE AUTHORISATION AND ACCREDITATION

16. To be authorised, accreditation needs to be in place. Accreditation forms the baseline upon which authorisation follows.

4 THE SCOPE OF THE AUTHORISATION

17. The NCCA specifies the ICT product categories and protection profiles to which the authorisation extends: see Article 21 (4) first sentence Commission Implementing Regulation (EU) 2024/482. The NCCA therefore should make publicly available a list of ICT product categories and protection profiles. The list should be maintained. Based upon this list the CB and ITSEF can indicate for which ICT product categories and protection profiles they wish to apply for authorisation.

18. In some specific situations applicable EU law or EU law implemented by national law may impact authorisation requirements for a specific certification of an ICT product or protection profile. Where this applies, the NCCA should provide and make publicly available additional information and guidance for the authorisation application.

19. If the CB or ITSEF is authorised for a specific ICT product category or protection profile, it may consider to extend the authorisation with a new ICT product category or protection profile by filing a new application. The NCCA should in this case indicate to what extent relevant, recent evidence can be re-used and what evidence needs to be provided[6]. The evidence for re-use needs to be relevant, in the sense that it is referring to an unchanged, still fully applicable situation and related to recent activities. In this case, a preparatory contact/meeting(s) with the NCCA may be useful before filing the application. The NCCA should indicate the planning, specify the foreseen procedure and provide an indication of the timelines.

4.1 ACTORS, THEIR ROLE AND THEIR LOCATIONS

20. Actors[7] involved in the authorisation are:

    a) the monitoring and supervising national cybersecurity certification authority (NCCA)
    b) the accredited or to be accredited CB
    c) the accredited or to be accredited ITSEF
    d) any possible entity that is subcontracted to the NCCA, CB or ITSEF

21. Actors mentioned in this document that either are in the preparatory process of their first authorisation or, want to renew their authorisation should consider using this guidance document.

4.1.1 The role and obligations of the NCCA

22. According to Article 60 (3) CSA and Article 21 (1) EUCC the monitoring and supervising body of the NCCA is responsible for the performance of the authorisation procedure of CBs and

[6] The Articles 21(2) - authorisation for CBs, and 22 (3) - authorisation for ITSEFs, of Commission Implementing Regulation (EU) 2024/482 provide the sources of re-use of documentation.

[7] For reasons of clarity: in order to get accredited, there is a separate State-of-the-Art document (SoA) developed for the CB and one for the ITSEF. They are listed under Annex 1 of EUCC.

ITSEFs and the compliance monitoring and supervision in the Member States where the CBs and ITSEFs are established. This implies that the NCCA is the party that is:

a) Processing the applications for authorisation;
b) Defining the scope for authorisation, meaning that the NCCA needs to specify the ICT product categories and protection profiles to which the authorisation extents;
c) Responsible for the planning, performance and documentation of the authorisation assessment which shall include at least structured interviews and a review of at least one pilot certification performed by the certification body/ one pilot evaluation performed by the ITSEF in accordance with EUCC requirements and may include:
    I. A demonstration of selected testing and related evaluation activities or certification activities;
    II. Performance of 'on-site' observations, audits or specific visits;
    III. Performance of (selected critical or specific) IT (system) audits (this may relate to use of AI systems or applications, network separation, etc.) or other specific information protection related audits in combination with document review;
    IV. Any request for assessment of specific internal and/or external audit reports demonstrating compliance, or;
    V. Requests for specific lifecycle-based assessments of use of assessment systems, applications or material or specific tools used in testing and related evaluation or certification activities;
d) Responsible for the performance of a review of a pilot certification by the CB;
e) Drafting and issuing the authorisation report and registering it;
f) Responsible for the authorisation decision;
g) Responsible for the performance of re-authorisation in the situation that changes occur which affect the authorisation;
h) Responsible for the performance of regular compliance audits.

23. To ensure a successful application, it is of importance that all actors involved in the authorisation procedure should have a thorough insight and understanding of the necessary preparations they need to make, know the steps in the procedure and have a view on the estimated timelines. The NCCA should ensure amongst others that the applicant:

a) has access to the information related to the application of authorisation;
b) knows what information is required for the application;
c) has access to the relevant guidelines and recommendations that are developed by the NCCA for successful application;
d) Knows how to use the correct system for securely exchange the necessary data with the NCCA;
e) Where the NCCA provides the opportunity to have a preparatory/informative meeting, organises workshops or webinars, the necessary information for these informative meetings should be made available as well. Such meetings should support all actors in finetuning the understanding of the whole procedure, its foreseen general planning and to ensure that all prerequisites are in place to smoothen the procedure and to ensure effective communication during the authorisation procedure.

Under Annex I, a detailed overview is provided of all relevant information that the NCCA should take into account.

24. The authorisation procedure can be started the moment the NCCA is indicating that they are ready to start the application procedures. From practical perspective, the readiness implies that the NCCAs should be able to:

a) Have their authorisation procedure digitally available;

b) Provide all the necessary information to ensure that CABs are well informed to prepare, plan and apply;
c) Start the application procedure;
d) Ensure that they have the necessary staff (internal or external), consisting of amongst others but not limited to: administrative & IT staff, assessors, subject matter experts/auditors and observers;
e) Ensure that they have the expertise to process the applications, provide the necessary information on the application for authorisation, guidance, the planning of the authorisation, the performance of the procedure, the documentation and retention procedures of the authorisation (this includes the provision of an authorisation report),
f) Perform quality management of the authorisation procedure that would possibly rely on internal review and improvements of the procedure;
g) Have a complaints procedure in place in accordance with Article 58 (7) (f) CSA, including a quality management system to ensure proper application and implementation, to perform regular audits/evaluations of the procedure, including an improvement cycle and a system to register the cases and the decisions taken related to authorisation complaints;
h) Have an concept agreement in place and a procedure in place to: i) request the participation/observation in the authorisation assessment of the NCCA in the country where an ITSEF is established and is subcontracted to a CB in its territory and ii) to request the support of the NCCA in the country where the ITSEF is located to use their monitoring and supervising powers under article 58 (8) CSA where this is seen as necessary and iii) to inform the manufacturer/developer that is participating the pilot certification of the participation in the authorisation assessment by the NCCA where the ITSEF is established;
i) Have the notification procedures in place in accordance with Article 61 CSA, and Articles 23 (notification of CBs) and 24 (notification of ITSEFs) EUCC[8].
j) Have the technical and organisational measures (TOMs) in place to ensure adequate protection of sensitive and confidential information and to securely exchange this type of information to other NCCA's and other relevant market surveillance authorities in accordance with Article 43 EUCC and the TOMs in accordance with Article 21 NIS 2.

4.1.2 The role of the CB and its establishments

25. The CB is the overall responsible body for the certification of the ICT product or protection profile. The certification body and the ITSEF can be separate departments or organisational units of one legal entity that performs all conformity assessment activities. The CB may also subcontract the ITSEF, being a separate legal entity, to perform the ICT product evaluation or protection profiles evaluation activities, or to assess in a compliance procedure if a sample or samples of the category of ICT products/or the protection profile is/are actually meeting the applicable requirements.

26. The CB shall be subject to authorisation by the NCCA in the Member State where it is established and issues certificates under assurance level 'high'. Where the CB has several establishments that issues certificates under assurance level 'high' in the same Member State, then each of the CBs should be subject to the authorisation assessment. Where processes, procedures and related documentation are used by several establishments of the CB, they may re-use evidence for their authorisation. Where a private CB performing activities by general

[8] This implies that notification needs to be send to the Commission of the European Union and to ENISA for the purpose of making available all information necessary for the effective operation of the scheme (see Article 23 (4) of Commission Implementing Regulation (EU) 2024/482.

delegation or by prior approval[9] has establishments in different Member States, it should be subject to authorisation by the NCCA in the country where it is established, regardless whether it performs the same certification activities or where these certification activities are different of scope, nature and extent. Where processes, procedures and related documentation are used by several establishments of the CB, they may be re-used for evidence.

27. Under assurance level 'high' there are several options for Member States to appoint a CB:
    a) The certification body of the national cybersecurity certification authority[10];
    b) The CB that is appointed by the delegating body to issue certificates by general delegation (Art 56 (6) (b) CSA. This CB can be a private of public body;
    c) The CB that performs certification conformity assessment activities and issues certificates upon prior approval of the prior approving body according to Art 56 (6) (a) CSA. This CB can be a private or public body.
28. All these bodies shall be subject to authorisation. The NCCA shall ensure that a CB which has received delegation only issues certificates in line with its scope of authorisation. The NCCA shall only give prior approval to certificates issued by a CB according to its scope of authorisation.

4.1.3 The role of the ITSEF and its establishments

29. The ITSEF is responsible for the performance of the ICT product testing and related evaluation activities and/or, where in scope of the authorisation, responsible for the specific testing and evaluation activities performed for protection profiles. In both cases it is also responsible for the assessment of the sample products to see if these meet the certification requirements of the protection profile or ICT product[11]. If any of these activities are performed by subcontracted party, the ITSEF shall be responsible for the activities performed by this third party as well. Therefore, the ITSEF should ensure that within the scope of authorisation defined by the NCCA in accordance with Article 22 (5) of EUCC, all tasks, activities and responsibilities performed by the ITSEF and the subcontracted party are clearly described and documented.

30. Where the ITSEF is performing conformity assessment activities for more than one CB which are all located in the same Member State, it should clearly indicate and specify the tasks, activities and responsibilities performed for each of the CBs it is sub-contracted to and where these CBs are located. If the scope for authorisation differs for each of its subcontracted services to the CBs, the NCCA should provide to the ITSEF an authorisation report for each of the subcontracted activities for the different CBs. Where activities of the ITSEF for each of the CBs it is subcontracted with overlap fully or significantly, the NCCA may decide to perform the authorisation of the ITSEF in a combined assessment, allowing the ITSEF to re-use the evidence of the CBs it is subcontracted with. In the case of significant but not full overlap, the NCCA may decide to re-use most of the evidence and add structured interviews and/or pilot evaluation specific audits for the not overlapping activities to reduce the workload for all related parties in the authorisation.

31. Where a ITSEF has establishments in different Member States and is subcontracted by CBs in these different Member States, each establishment of the ITSEF should be subject to authorisation by the NCCA in the Member State of its establishment, regardless whether it

[9] Under Article 56 (6) CSA the NCCA has the choice to either delegate the certification activities or partially delegated some of the certification activities by using a prior approval model.

[10] This body should be compliant with Art. 58 (3) CSA.

[11] See Article 25 (2) (c) and Article 25 (3-9) EUCC.

performs the same activities or were these activities are different of scope, nature and extent. Where processes, procedures and related documentation are used by several establishments of the ITSEF, they may be re-used for evidence in line with chapter 4, point 19.

32. If the ITSEF performs activities for a CB in another Member State than where it is established, and it does not perform conformity assessment activities for a CB in its country of establishment, it should notify this to the NCCA of the country of its establishment. Unless a bilateral agreement is in place, the responsible NCCA for all authorisation matters is the competent one designed by the Member State in which the ITSEF is established. A bilateral agreement may however be established if the NCCA in which the ITSEF is established wishes to rely on the expertise of the NCCA where the ITSEF operates as a subcontractor of CBs. This bilateral agreement could allow the two NCCAs to participate in the authorisation of the ITSEF. The reason for this combined authorisation by two NCCA's is related to the fact that the NCCA in the Member State of the CB can only monitor the activities of CABs in their own Member State, they do not have extra-territorial competency. The NCCA in the Member State where the CB is located is unable to monitor and supervise the ITSEF which is located in another Member State. It should reach out to the NCCA in the Member State where the ITSEF is located and request for observing support and should be involved in the authorisation assessment. A combined authorisation assessment team should be set up. The NCCA of the Member State where the CB is established issues the authorisation report, takes the decision to authorise the ITSEF and is the responsible authority for monitoring and supervision. Where there is a need to use monitoring and supervising powers in accordance with Article 58 (8) CSA towards the ITSEF, it should request the NCCA of the Member State where the ITSEF is located to use its legal powers. The notification of the authorisation to the Commission should be performed by the NCCA where the ITSEF is established and should provide a copy to the NCCA where the CB is established. The notification is based on the decision taken by the NCCA of the Member State in which the CB is established.

33. If the ITSEF is performing the exact same activities (same scope for authorisation) for a CB in the Member State of its establishment and for a CB established in another Member State, it will face two authorisation procedures in these Member States, but should be able to reuse evidence for the authorisation. This is due to the fact that there are different NCCAs and CBs involved and the subcontracting conditions may be different[12]. As the authorisation reports of both NCCA's are subject to peer review, both NCCAs should collaborate related to their authorisation and monitoring & supervising activities to the extent they deem appropriate. Where an NCCA plans to decide to change a status in authorisation upon performance of re-authorisation or an authorisation compliance audit[13], it should notify the NCCA in the other Member State and provide the reasoning of its planned decision as this may impact the status of the authorisation in the other Member State.

5 SUBCONTRACTING THIRD PARTIES BY CB AND ITSEF

34. Both the CB and the ITSEF may decide to subcontract a third party (this needs to be a legal entity) to perform some of its conformity assessment activities. Where this occurs, these third-party services are also subject to the authorisation of the CB or ITSEF for which they perform their subcontracted services. This implies that for their provided services they should provide the following information necessary for authorisation, renewal of authorisation and compliance audits that are planned by the NCCA, which is related to:

[12] In some Member States national law may also influence the authorisation.

[13] For the re-authorisation procedure chapter 8, paragraph 8.1 should apply, for the compliance audit chapter 9 should apply.

a) the actual overview of the technical competences for the services they provide;
b) the (secure) exchange of information and organizational and contractual aspects of their collaboration with the CB or ITSEF they are subcontracted to;
c) information on the TOMs they need to have in place and demonstrate the related technical competences.

35. Key critical roles/functions require a proper competence management strategy related to continuity of the available technical competences for the provided services. This implies that the key competences should be identified and managed accordingly. In this respect, the contracting with external experts should be described, as well as the level of dependency on these externals. The overall succession planning of internal and contracted external staff as well as the related learning & development planning should ensure the continuity of the required technical competences and should therefore be subject to the authorisation assessment by the NCCA. All these elements (this includes point 19 and 18) should be subject to the competence management system of the CB and ITSEF and should be subject to applicable quality management.

36. The CB and ITSEF also should be aware of the fact that the parties they subcontract play an important role in the chain of compliance in the sense that any non-compliance from the side of the subcontracted party may have consequences for the authorisation (and accreditation) of the CB or ITSEF that subcontracted them. The requirements related to the technical competences and the TOMs[14] should equally apply for the activities performed by the subcontracted parties.

37. In accordance with point 9 of the Annex of the CSA it is the CB that legally has the overall responsibility and liability for the performance on all conformity assessment activities to be performed to certify the ICT product. This implies that the CB needs to ensure compliance of the conformity assessment activities and reviews ex-ante if all procedures are followed before a certificate will be issued under its responsibility. In this respect, it may:

    a) perform or request regular compliance audits;
    b) request the necessary evidence to ensure overall compliance;
    c) request to support in the preparation of the (re- or renewal) authorisation related to the ITSEF conformance assessment activities that are subject to the subcontracting by the CB.

38. These elements are to be reflected in the sub-contracting and checked by the NCCA when it comes to authorisation.

6 THE AUTHORISATION

6.1 THE PLANNING OF THE AUTHORISATION BY THE NCCA

39. The application by the CB or ITSEF should include all the necessary documentation and the NCCA will check if all necessary documentation is provided and upon the confirmation that all documentation is provided will send out an authorisation planning within a reasonable time before the actual start.

[14] See chapter 11.

40. The NCCA may plan a kick-off meeting to support the planning of the ITSEF and the CB authorisation procedure. The authorising NCCA should provide to the audited entity a draft planning that consists of:

    a) The document review upon completeness and content;
    b) The selected authorisation team including an overview of the planned assessors/evaluators/auditors/experts/observers that participate in the authorisation procedure and what assessment activities they will perform;
    c) The structured interviews for the assessment of the technical competences, cooperation activities between the ITSEF and the CB and the implementation of TOMs;
    d) The assessment activities to be performed for the pilot certification;
    e) Where applicable, any other foreseen relevant supporting assessment activities as described under paragraph 4.1.1 point 22 (c).

41. The NCCA should ensure that the assessors/evaluators/auditors/experts/observers that are selected for the performance of the authorisation assessment by the NCCA (the NCCA authorisation assessment team) have:

    a) The appropriate technical expertise related to the scope of the requested authorisation;
    b) The competences to perform an assessment[15];
    c) A high level of integrity, professionalism, ethical-, social- and business values;
    d) An impartial working attitude;
    e) The technical competences to work with and protect sensitive and confidential information;
    f) The appropriate screening reducing the chances of fraud, corruption, spying, leaking confidential and sensitive information.

6.2 THE AUTHORISATION ASSESSMENT

6.2.1 The ITSEF documentation & technical competences to be assessed by the NCCA

42. The necessary documentation provided by the ITSEF for authorisation should at least comprise the information that it provided to the NAB for accreditation[16]. The NCCA should rely on the assessment of these documents performed under the accreditation. As accreditation is the baseline for authorisation, a copy of these documents should be made available by the applicant to the NCCA as well as the evidence listed in Annex I for the purpose of having the correct context necessary for effective monitoring and supervision of the additional and specific requirements that are subject to authorisation. This documentation consists of the ITSEFs organisation structure that should entail at least a description of those elements that fall under the scope of authorisation:

    a. The ICT product categories and protection profiles for which the authorisation is requested (scope of authorisation);
    b. The strategic organisational plans related to the scope of authorisation;
    c. The top management and its responsibilities,

[15] To perform structured interviews, or audits effective interaction with staff of ITSEF and CB is necessary requiring both technical and social competences from the NCCA assessment team.

[16] This information is likewise required for accreditation and can be a copy. It is the NAB that assesses these documents under accreditation.

d. The resources, and the competence management system the key critical roles[17] and financing of the roles;
e. The departments performing the day-today business and their responsibilities;
f. The technical management providing an overview of the technical conformity assessment operations (this includes the IT & OT responsibilities and systems used & their architecture and the related dependencies on third party service providers),
g. The roles/functions that have the responsibility for the technical competence management and their succession planning;
h. The quality management, ensuring that all policies, procedures and measures are in place & retained according to retention policies[18] and are regularly evaluated and audited, and subject to a PDCA cycle[19];
i. The compliance management, including the procedures for handling of correction of non-conformities and non-compliances;
j. The cybersecurity management of the ITSEF that has a position in the top management with the cybersecurity responsibility and authority to define and implement the required policies and procedures and technical and organisational measures (TOMs) for effective information protection of sensitive and confidential information as well as to exchange this type of information with their CB, customer, and where applicable with the NCCA;
k. Any subcontracting or hiring of external staff by the ITSEF for its activities are to be described and related contractual responsibilities need to be provided and include the overall responsibility of the ITSEF. The ITSEF sees to it that externals meet the authorisation requirements of the ITSEF for the subcontracted or hired services;
l. The financial information related to the ITSEF organisation, providing information on the financial resources including an overview of the financial dependencies and foreseen financial risks, the resources spend on maintenance of staff competences including learning and development, the resources spend on the cybersecurity including the technical and organisational measures related to information protection and cybersecurity training of staff.

43. The ITSEF should demonstrate its technical competences and expertise and specify them in documentation to be provided to the NCCA for each of the evaluation activities that are performed by its internal and external staff within the defined scope of authorisation. This documentation should comprise a description of the internal evaluation methods and tools of the ITSEF. Operating under assurance level 'high' implies that the ITSEF shall be able to determine the resistance to state-of-the-art cyberattacks carried out by actors with significant skills and resources. A mapping should be provided in how the staff members meet the required technical competences. The business resume/CV or an overview providing equivalent information should reflect the obtained technical competences of the staff /hired personnel based upon their latest appraisal. A possible example template of this mapping is provided in Annex V.

44. The list of technical competences that at least should be subject to authorisation, is provided under Annex II. Based upon the scope of the authorisation and the related evaluation activities, the NCCA may require additional relevant technical competences that the ITSEF should demonstrate. The technical competences that are assessed should be listed in an annex to the authorisation report.

[17] As described under chapter 5 point 34 and 35.

[18] See Article 40 EUCC.

[19] A Plan-Do-Check-Act cycle, which is a continuous improvement cycle.

6.2.2 The CB documentation & technical competences to be assessed

45. The necessary documentation provided by the CB for authorisation should at least comprise the information that it provided to the NAB for accreditation[20]. The NCCA should rely on the assessment of these documents performed under the Accreditation. As accreditation is the baseline for authorisation, a copy of these documents should be made available by the applicant to the NCCA as well as the evidence listed in Annex I for the purpose of effective monitoring and supervision of the additional and specific requirements that are subject to authorisation. This documentation consists of the CBs organisation structure that should entail at least a description of those elements that fall under the scope of authorisation:

    a) The ICT product categories and protection profiles for which the authorisation is requested (scope of authorisation);
    b) The strategic organisational plans related to the scope of authorisation;
    c) The top management and its responsibilities,
    d) The resources, and the competence management system the key critical roles[21] and financing of the roles;
    e) The departments performing the day-today business and their responsibilities;
    f) The technical management providing an overview of the technical certification operations (this includes the related IT & OT responsibilities and systems used & their architecture and the related dependencies on third party service providers);
    g) The roles that have the responsibility for the technical competence management and their succession planning;
    h) The quality management, ensuring that all policies, procedures and measures are in place & retained according to retention policies[22] and are regularly evaluated and audited, and subject to a PDCA cycle[23];
    i) The compliance management, including the procedures for handling of correction of non-conformities and non-compliances;
    j) The cybersecurity management that has a position in the top management with the cybersecurity responsibility and authority to define and implement the required policies and procedures and technical and organisational measures (TOMs) for effective information protection of sensitive and confidential information as well as to securely exchange this type of information with their ITSEF including the forms of cooperation, with the customer, and where applicable with the NCCA;
    k) Any subcontracting or hiring of external staff by the ITSEF for its activities are to be described and related contractual responsibilities need to be provided and include the overall responsibility of the ITSEF. The ITSEF sees to it that externals meet the authorisation requirements of the ITSEF for the subcontracted or hired services;
    l) The financial information related to the CB organisation, providing information on the financial resources for the elements that are subject to the scope of authorisation, including an overview of the financial dependencies and foreseen financial risks, the resources spend on maintenance of staff competences including learning and development, the resources spend on the cybersecurity including the technical and organisational measures related to information protection and cybersecurity training of staff;

[20] This information is likewise required for accreditation and can be a copy. It is the NAB that assesses these documents under accreditation.

[21] As described under chapter 5 point 34 and 35.

[22] See Article 40 EUCC.

[23] A Plan-Do-Check-Act cycle, which is a continuous improvement cycle.

46. The document review is focussing on the necessary content that needs to be mature and to the point, providing a clear overview of the activities, responsibilities and the related technical competences. Where updates, corrections or clarifications are considered necessary, a second review may be necessary depending on the extent, nature and impact of the findings.

47. Operating under assurance level 'high' implies that the technical competences should be in place to be able to perform the certification activities in a context where certification focusses on the determination of the resistance to state-of-the-art cyberattacks carried out by actors with significant skills and resources. A mapping should be provided in how the staff members meet the required technical competences. The business resume/CV or an overview providing equivalent information should reflect the obtained technical certification competences of the staff /hired personnel based upon their latest appraisal. A possible example template of this mapping is provided in Annex V.

48. The specific technical competences for certification activities should focus amongst others on the ability to review, assess and validate amongst others, but not limited to:
    a) The work of the ITSEF performed under assurance level 'high' for the authorisation scope, including the analysis, and review of the Evaluation Technical Report,
    b) The drafting the certification report (including the sanitization of a security target in accordance with Annex V, section V.2 EUCC),
    c) The task to analyse, process and document the findings and to provide technical and procedural recommendations related to the evaluation activities performed by the ITSEF,
    d) The task to make certification decisions related to issuance of certificates, suspensions, restrictions and withdrawal in accordance with the procedures, and to monitor the conditions for issuance of an EUCC certificate;
    e) Handle the procedures related to: vulnerability handling and patch management; handle the assurance continuity; the compliance monitoring and complaints;

49. Where the CB is using the services of third parties[24], the CB should provide to the NCCA all information demonstrating its technical competences and expertise and specify this for each of their certification activities that are performed by the third party within the defined scope of authorisation. This implies that:
    a) An overview of the technical competences that are used by means of subcontracting or hiring of external staff /delegation/prior approval details should be provided. The CB should see to it that externals meet the authorisation requirements of the CB for the subcontracted or hired services;
    b) The overview of the TOMs and the related technical competences to implement and maintain the TOMs, including the legal overall responsibility for its compliance for the CB.

50. The CB should demonstrate it conducts its activities in cooperation with an authorised ITSEF by providing a proof of the subcontracting contract addressing:

    a) The exchange of information and the conditions that apply[25];
    b) The documentation describing the means and aspects/fields of cooperation;

[24] Third parties can be entities providing services or hired external staff.

[25] For exchange of sensitive or confidential information secure systems need to be used. Where the CB is certifying an ICT product of which components have been certified, the ETR of the components may be reused but should only be shared upon prior approval of the 'component certification customer' (the holder of the certificate on the component).

c) The documentation on the procedure for re-use of evidence from existing authorisations, including where applicable evidence for extending the authorisation in line with chapter 3, point 19 coming from another CAB, which includes a description of how this information is exchanged and under what conditions;
d) The documented right of the CB to request information and visit the ITSEF for the purpose of the certification decision;
e) The elements of cooperation on behalf of compliance activities of the certified product (e.g., activities related to Article 26 EUCC for which it reaches out for support of the ITSEF; the request by the CB to the ITSEF for the support in a sampling procedure; or support in the vulnerability handling procedure;
f) The collaboration with the ITSEF in the assurance continuity procedure described under Annex IV of EUCC.

51. Where the CB uses third parties that for the performance of their services cooperate with the ITSEF, these services should be described and where applicable meet the requirements under point 49.

6.2.3 Additional assessment activities

52. It may occur that during the authorisation procedure additional material, documentation or clarifications or additional assessment activities are necessary for the NCCA authorisation team. They will for this purpose make comments, pose requests, plan additional meetings and/or assessment activities. In this sense the provided planning by the NCCA is to be seen as a guideline for the conformity assessment body. The conformity assessment body is allowed during the authorisation procedure to make clarifying comments, ask clarifying questions, provide where allowed or requested by the NCCA authorisation team relevant supporting and clarifying documentation. The NCCA authorisation team should ensure that all assessment activities are well documented and include:
    a) Any clarifications provided during the assessment activity;
    b) The date, time and location of the assessment activity;
    c) The name(s) of the NCCA authorisation team members being either or assessors/evaluators/auditors/experts/observers that were present during the assessment activity, as well as the present, selected staff member(s) of the conformity assessment body under authorisation.

53. All documentation received from the applicant, including the additional information received during the application, should be registered[26] including date of receival by the NCCA authorisation team and serves as the evidence upon which the authorisation report is to be drafted. The report therefore should for each of the findings refer to the registered information number. Upon the received information, it should not be allowed to change any of the information and it should be securely stored and retained in accordance with the appropriate NCCA rules[27]. The information should only be made accessible upon a direct need-to-know basis.

54. Where during the authorisation assessment some major non-conformities are identified, the CB or ITSEF should resolve these upon the instructions of the NCCA authorisation team and propose the resolutions to the NCCA authorisation team for review within the provided timeline.

[26] The registration under the authorisation file of the CB or ITSEF should consist of a short description of the evidence with an associated evidence number.

[27] The NCCA is considered to be subject to the NIS2 directive, meaning that the Member State where the NCCA is established should define such rules in accordance with Article 21 NIS2; these rules could be part of the peer review mechanism.

Where more time is required to resolve the matters, the CB or ITSEF may request for this. Where the non-conformities are seen as minor, a corrective plan should be developed by the CB or ITSEF and it should provide the plan together with necessary evidence to the NCCA authorisation team that the minor non-conformities are being handled. The NCCA authorisation team should approve the corrective plan.

6.2.4 The pilot evaluation.

55. The ITSEF and the CB (in the case of the prior approval model this may be with the involvement of the NCCA, as provided under point 58) should jointly prepare and design the planning for the pilot evaluation, based upon and in close collaboration with a contracted customer that intends to undergo a pilot certification procedure for its ICT product or protection profile in accordance with EUCC.

56. The identified customer should be made aware by the CB of the pilot evaluation risk, meaning that the authorisation) requires a positive outcome and a positive result on the accreditation in order to transform the pilot certification into a formal certification. The necessary contract with the customer should be in place and include the conditions that apply for the transformation of the pilot evaluation to an EUCC certification. Where the ITSEF is located in another Member State than the CB, the necessary contractual clauses need to indicate the rules related to Chapter 4, paragraph 4.1.3, point 32.

57. The ITSEF should, upon written approval of the customer, send the evaluation plan to the CB for approval. The CB should establish for the purpose of the pilot a certification plan and send it together with the evaluation plan for approval to the NCCA. Testing and related evaluation activities and certification activities should be described in terms of methods, use of tools and procedures used and provide the location of the planned activity, as well as the planned timelines for these activities that need to be realistic and proportionate for the related activity, and include the planning of the necessary staff (business resumes need to be included) for each of the activities. Any foreseen re-use of evidence based upon Article 22 (3) EUCC should be explained and included/attached in the related evaluation plan. Any foreseen re-use of evidence based upon Article 21 (2) EUCC should be explained and included/attached in the certification plan.

58. The evaluation and certification plans should serve as input for the selection of the NCCA assessment team that will perform the structured interviews and other applicable assessment activities (as described under chapter 4, paragraph 4.1.1, point 22 (c). for the pilot certification. The pilot certification should follow all the aspects of the EUCC. Re-use of evidence should be based upon Article 21 (2) EUCC for the CB and for the ITSEF Article 22 (3) EUCC applies.

7 THE AUTHORISATION REPORT

59. When all assessment activities are performed, the NCCA authorisation team should draft for each assessment activity performed the elements of the authorisation report as described under Annex III. To ensure that all elements are correctly related and integrated the NCCA should appoint the person responsible for the final draft who should be responsible for the coordination of the authorisation assessment activities in a way that the authorisation report is: consistent, coherent based upon the facts and findings provided by the registered information and does not include presumptions, suggestions or non-founded estimations.

60. The authorisation report should be signed by the legal representative of the NCCA and should be sent without undue delay to the applicant (the CB or ITSEF) after registration of the report.

In the case of general delegation, the delegating body should receive a copy of the report. In the case of prior approval, the prior approving body should receive a copy.

61. The NCCA should see to it that the information necessary for the notification for authorisation as described under Article 23 and 24 EUCC is provided without undue delay after the authorisation is performed and the report is registered, to:

    a. the European Commission for the purpose of notification in accordance with Article 61 of the CSA and Article 23 and 24 EUCC;
    b. ENISA, to allow the publication of the authorisation of the ITSEF on the EU Cybersecurity certification website. The executive summary, the conclusions and verdict are to be made public with the unique registration number.

62. The unique registration number of the authorisation report should consist of: the abbreviation of the NCCA name and EU country abbreviation, the date of authorisation, and the abbreviation of the authorised CAB. The NCCA may add any other information to the registration number it deems necessary.

63. The report is subject to peer-review of NCCAs in accordance with Article 21 (3) EUCC.

8 CHANGES AFFECTING THE AUTHORISATION: RE-AUTHORISATION

64. After authorisation, the CB and/or ITSEF may face changes that affect or have an impact on the authorisation requirements and which may be very different in extent, duration and nature. For this reason, the NCCA needs to have a procedure in place that allows the NCCA to decide upon the occurring changes to start a review of the authorisation. Some examples of changes affecting the authorisation could be:

    a) Organisational changes in the (legal) structure: such as a merger of two CBs or ITSEFs or a takeover, the setting up of a joint venture, a split in the existing organisation or management buy-out. The technical competences and TOMs due to these changes may need to be reviewed as the operational environment changes and responsibilities may be shifted or moved to another organisation that is not accredited and authorised. National law related to foreign investments may apply and needs to be taken into account by the NCCA in respect of the applicable TOMs and technical competences related to information protection. This may also impact accreditation;
    b) Technical changes due to new IT systems, new tools, start or change in the use of AI in conformity assessment activities, changes in the certification activities or procedures or changes in the evaluation activities, or changes in the testing environment, changes in the available technical competences;
    c) The CB and/or ITSEF may decide during authorisation to outsource activities and subcontract a third party;
    d) Circumstances affecting the operation of the CB or ITSEF: they may face a (temporary) situation where they are unable to perform their tasks in unforeseen situations such as: floods, wildfire, earth quakes, or war, even if the business continuity procedure works, the actual ability to perform the work in the authorised environment may substantially change and therefore impact compliance to the requirements for authorisation;
    e) There may be circumstances that lead to a decision of the CB or ITSEF to stop their business, or a situation where the CB or ITSEF needs to stop its business (e.g., bankruptcy), or temporarily force the body to stop its activities for reasons of running investigations that require temporary closure/inactivity;

f) Changes in the scope of authorisation, for example in the case an ICT product reaches its end of life and is replaced by a newer version, or different product, with a different security posture, thus forcing the list of the categories of the ICT products or protection profiles to be updated.
g) New legislation be it national or EU law.

8.1 THE RE-AUTHORISATION PROCEDURE

65. The CB or ITSEF subject to the change needs to report without undue delay, after receiving information making the body aware of a change which is substantially affecting the requirements against which it was authorised. Upon the notification and background of the change, the NCCA re-authorisation team may start a re-authorisation procedure and:

a) request to perform an impact analysis and upon this analysis provide instructions to the conformity assessment body and propose appropriate remediating or new measures, or;
b) perform a document review and request the conformity assessment body to provide updated documentation, evidence or information for further review and assessment by the NCCA re-authorisation team, or;
c) decide upon the information received to (partially or in full) re-authorise and perform structured interviews, or perform other assessment activities described under chapter 4, paragraph 4.1.1, point 22 (c).

66. If minor non-conformities are found, the CB or ITSEF should develop a corrective action plan and show evidence to the NCCA re-authorisation team that the minor non-conformities are being handled. Where the ITSEF needs to draw up the corrective plan, it involves the CB in the proposed correction plan, if applicable.

67. If major non-conformities are found or the authorisation team considers that the scope of the authorisation of the ITSEF or CB must be modified, it should inform the ITSEF or CB accordingly. This information should include the scheduling of (targeted) audit activities and a maximum timeframe for the CB or ITSEF to take corrective actions. Upon the correcting actions, the NCCA re-authorisation team decides upon the scope and re-authorisation activities to be performed before finalizing the re-authorisation process.

68. These actions may lead to a new version of the authorisation report under the name of compliance audit authorisation report. The initial validity of the authorisation remains in place as the duration of the authorisation validity should not exceed the validity of the accreditation in accordance with Articles 21(4) and 22 (5) EUCC.

8.2 THE RE-AUTHORISATION REPORT

69. Where a re-authorisation takes place, the existing report will be updated under the name of re-authorisation report re-using the unique number of the initial report under a new version. The re-authorisation report will have an introduction which includes the reasons for the re-authorisation, and indicates the scope of the re-authorisation. Re-use of evidence is possible but this needs to be indicated and justified. Where elements of the initial authorisation report are not within the scope of re-authorisation this needs to be indicated. For the updated audit report elements, a new paragraph needs to be established under the indication of “re-authorisation”. Under this paragraph the new situation needs to be described and the findings need to be provided including any applicable comments of the CB and/or ITSEF.

70. The unique number of the report remains, but will be adding the abbreviation R-A (for indication of re-authorisation) and the applicable version number [“V.X”] at the end of the number. A new dedicated executive summary will be added under indication of “re-authorisation”. The report will be registered by the NCCA re-authorisation team. Depending on the nature and impact of

change and all circumstances at hand, the NCCA re-authorisation team may decide to suspend, restrict or even withdraw the authorisation, which will trigger a notification to the Commission in accordance with Article 61 (1) of the CSA and Articles 23 (CB) or 24 (ITSEF) EUCC as an updated report under new version.

71. The NCCA re-authorisation team may, given the circumstances at hand, also decide to inform the NAB where there are possible implications for accreditation.

9 COMPLIANCE AUDIT

72. The NCCA authorisation team should perform a compliance audit at least twice during the duration of the authorisation and preferably after 1,5 years of the start of the authorisation, to monitor the CABs in their compliance. During such audits the NCCA authorisation team should focus for this compliance audit in particular on:
    a) Whether the CAB still complies with this document's requirements and the obligations related to authorisation;
    b) The capability of the ITSEF or the CB to verify if the capability is not altered, for example, if a member of staff who holds a key technical knowledge leaves the CAB;
    c) The assessment of the technical competences of the ITSEF to perform the vulnerability handling procedure and the technical competences necessary for performance of the reviews by the staff of the CB. The NCCA authorisation team should be able to witness how the ITSEF team applies the vulnerability handling procedure, demonstrating the appropriate technical competences;
    d) That the information security is handled in accordance with the TOMs using the appropriate state-of-the-art technical competences in an adequate way;
    e) That (suitably selected) evaluators and certification decision makers have the state-of-the-art technical competences, e.g., by attending or organizing conferences, taking training courses, obtaining professional certifications, participating in workshops, research projects, challenge/simulation exercises, or similar activities;
    f) That the records and processes of the competence management system are up-to-date, include a succession planning and a sound learning and development planning with suitable budget and are aligned with the bodies' strategy;
    g) That the ITSEF and the CB use state-of-the-art and cybersecure equipment and methodologies to perform evaluations and allow certification decisions;
    h) The incident handling procedure and logs, documentation;
    i) The vulnerability handling of the ICT systems, services and tools in accordance with the information security management system.

9.1 THE AUTHORISATION COMPLIANCE REPORT

73. The report of the NCCA authorisation team on the compliance audit follows the methodology of the re-authorisation report as described under paragraph 8.2. The report has the name: "authorisation compliance report". The unique number of the report remains, but will be adding the abbreviation C-A (for indication of compliance-authorisation) and the applicable version number ["V.X"] at the end of the initial unique number. A new dedicated executive summary will be added under indication of "compliance audit". Where the compliance report leads to a change in status of the authorisation, a notification to the Commission in accordance with Article 61 (1) of the CSA and Articles 23 (for CB) or 24 (for ITSEF) EUCC will follow.

10 INFORMATION PROTECTION

74. The ITSEF and the CB operating under assurance level 'high' will assess ICT products used in high risk or critical areas for which there is a need to minimize the risk. The ITSEF will determine

the level of resistance to state-of-the-art cyberattacks carried out by actors with significant skills and resources which is verified by the CB. The information they collect, generate in the overall conformity assessment activities and store is confidential and sensitive information on the ICT products. This is not only information related to the conformity assessment, it also comprises intellectual property rights like business secrets, patents, copyright or commercially sensitive data like trade secrets and even the fact of application to the evaluation/certification procedure. These sources of information gathered, processed and stored are attractive to cyberattacks performed by high skilled attackers.

75. For this reason, it is of great importance that the CB and ITSEF take the appropriate Technical and Organisational Measures (TOMs) to minimize the risk of attacks and cyber incidents. Policies, procedures and processes need to be in place to detect, respond to, recover from these attacks or incidents and take measures that prevent these attacks or incidents from re-occurring. The protection of information is not only related to protecting information during the certification procedure, but also during the certification lifecycle and thereafter for the information retention duration. This implies also the cybersecure destruction of data at the moment of expiration of the retention time of conformity assessment documentation. For this reason, they need to meet high requirements in information protection and ensure that the proper TOMs are in place.

10.1 THE TECHNICAL AND ORGANISATIONAL MEASURES (TOMs)

76. Following factors should play a role in defining the appropriate TOMs for CBs and ITSEFs:

    a) The ITSEF subcontracted to the CB and working under its responsibility also should follow TOMs in accordance with Article 22 (1) (c) EUCC. Given the context of the relation and operation between the ITSEF and the CB this implies that the ITSEF should operate commensurable TOMs as the CB. The CB is only able to perform its activities upon the data provided by the ITSEF which means that they operate in the same environment.

    b) Article 51 CSA provides clear guidelines for TOMs that should be applied in European cybersecurity certification schemes for the lifecycle of certification and the retention period to achieve these objectives. They should cover the schemes related to certification of ICT products, ICT services and ICT processes, and should apply to the conformity assessment bodies.

    c) The ITSEF and CAB should operate a process for selection of TOMs that includes referring to established standards and tested/certified products where possible, and for regularly testing of the TOMs, where possible (e.g., checking for physical alarms, checking staff awareness or performing a penetration testing on the firewall).

77. The TOMs should meet the following requirements:

    a) They should be defined upon a risk assessment that should be performed by the CB and ITSEF and cover the degree of the entities' exposure to risks;

    b) They take the organizational context into account, i.e., TOMs possibly provided by a larger entity which the CB and ITSEF is part of;

    c) They should take into account the likelihood of occurrence of incidents and their severity, including their societal and economic impact;

    d) They should have an all-hazard approach that aims to protect their network and information systems and physical environment from incidents;

    e) They should be regularly audited/evaluated including an improvement cycle.

78. The TOMs that could apply are listed under Annex IV.

10.2 THE SPECIFIC COMPETENCES FOR INFORMATION PROTECTION

79. The competences for information protection should be related to all the roles /functions and responsibilities within the organisation and that of its subcontracted staff and should consider the different competence levels required. The template provided under Annex V could support in providing this overview to the authorisation team. Where TOMs apply, the role/function should include the related responsibility and the required competences. These competences should focus on the ability, knowledge and skills to effectively protect sensitive and confidential information by means of TOMs. This implies amongst others:

    a) The ability, knowledge and skills to perform a risk and impact assessment to derive the necessary TOMs;

    b) The ability, knowledge and skills upon threat analysis, to derive, evaluate, update and adjust the TOMs to the level appropriate to protect sensitive and confidential information and to report any necessary deviation with reasoning without undue delay to the policy responsible;

    c) The ability, knowledge and skills to implement, apply and assess the applicable TOM-policies in the role/function of the staff member;

    d) The ability, knowledge and skills to effectively protect the information in and outside work environment and during travel in line with the confidentiality & communication protocols/policy;

    e) The ability, knowledge and skills to recognize and report any signs of IT system or tool compromise and to act in accordance with reporting and handling of incident- & vulnerability handling procedures and were necessary take appropriate remediating actions;

    f) The ability, knowledge and skills to support, educate and/or train, correct and encourage other colleagues, customers and facility visitors in the correct application of the TOMs that are in place;

    g) The ability, knowledge and skills to carefully balance and manage the need in (on-site) audits to request the access to (sensitive or confidential) information necessary for authorisation and to respect the site information security requirements in a customer friendly manner;

    h) The ability, skills and knowledge to keep integrity and impartiality under all circumstances and support, educate and/or train, correct and encourage other colleagues, customers and facility visitors in the correct application of the high standard of integrity and impartiality in relation to the handling and protection of sensitive and confidential information.

11 THE AUTHORISATION DURATION, VALIDITY & DECISIONS ON STATUS

11.1 THE VALIDITY

80. The duration of the validity of the authorisation in general should follow the validity of the accreditation[28]. However, this may become different when the authorisation is subject to a change, or it faces a non-compliance and leads to a withdrawal of the authorisation. If the accreditation of a CB or ITSEF during its initial validity is subject to changes or non-compliance that will lead to a withdrawal of the accreditation, the authorisation is also withdrawn, as accreditation is a requirement for authorisation. The same situation could apply for a restriction

[28] See Article 21 (4) EUCC.

decision. For this reason, the NAB and NCCA should inform each other well when changes or non-compliances occur.

81. If changes in the requirements for accreditation lead to a re-accreditation, the NCCA may decide to suspend the authorisation until the re-accreditation is finalised with a positive verdict on the accreditation. If the re-accreditation leads to a new validity of accreditation, the NCCA may decide to proceed to an audit of the CAB after re-accreditation, and the validity of authorisation after suspension should be adapted according to Art. 21 (4) and Art. 22. (5) EUCC. In these circumstances, the NAB and NCCA should inform each other well and in a timely manner.

82. If the authorisation validity of a CB or ITSEF expires and no new application is filed, the NCCA should inform the CB or ITSEF in a timely manner about deadlines to ensure an application for re-authorisation. After receiving the application for re-authorisation the re-authorisation audit should be performed by the NCCA. The re-authorisation team should assess that the CB or ITSEF have taken all measures necessary to ensure that their customers are informed and running evaluation and/or certification procedures are closed. The re-authorisation report procedure under chapter 8 paragraph 8.2 should apply. The expiration of the authorisation triggers Article 61 (1) CSA and the NCCA should notify the Commission in accordance with the Article 23 (for the CB) or Article 24 (for the ITSEF) EUCC.

11.2 THE DECISIONS ON THE STATUS OF AUTHORISATION

83. According to article 61 (1) CSA the NCCA shall notify the European Commission of any subsequent changes in the status of accreditation and authorisation. Therefore, the NCCA should ensure that the NAB informs the NCCA in all cases of change in status. These changes in status should be reported by the NCCA to ENISA for publication on the European Cybersecurity Certification website without undue delay after the decision was taken by the NCCA in accordance with Article 23 (4) EUCC or received from the NAB.

84. The suspension is by nature a temporary status that usually implies that a re-authorisation procedure is taking place to address changes and non-conformities. For this reason, this status has no impact on the validity nor the duration of the validity of the authorisation.

85. The status of restriction may have a short term or more mid to longer term character, depending on the circumstances. A CB or ITSEF may decide to limit the scope of authorisation and stop their activities for certain categories of ICT products or protection profiles. Also, the NCCA may restrict the scope of authorisation based upon a non-compliance. The CB or ITSEF can only perform its conformity activities for the limited scope for authorisation. The NCCA should indicate the reasons for restriction. If the decision is taken based upon a compliance audit, the reasoning should be provided in the authorisation compliance report in the section of the decision. Where the CB or ITSEF indicated to limit their scope upon own initiative, the reasoning should be provided in a re-authorisation report in the section of the decision.

86. For reasons of proper functioning of the certification market and legal certainty, it is important that applications or holders of certificates know if the CB and/or ITSEF have restrictions and are not able to perform certain conformity assessment activities for certain ICT products and/or protection profiles that are subject to the restriction. If re-certification, vulnerability handling procedure or assurance continuity procedure of these certified ICT products and/or protection profiles lead to problems, due to the restriction decision, the NCCA may request the holder of the certificate to engage with another authorised CB and/ or ITSEF to perform these activities and the holder of the certificate that want to have its ICT product of protection profile recertified may turn to another CB and/or ITSEF. In that case, the initially authorised CB and/or ITSEF should collaborate in sharing the necessary evidence and certification documentation for the purpose of the re-certification, vulnerability handling and assurance continuity.

87. Where a request is received by the NCCA of a CB and/or ITSEF to stop its activities chapter 8, paragraph 8.1, point 65 applies. The NCCA should assess if the CB or ITSEF has taken all measures necessary to ensure that their customers are informed and that the running evaluation and/or certification procedures are either closed or transferred to another conformity assessment body that is authorised for the applicable scope and shall withdraw the authorisation in accordance with Article 61 (1) CSA and the applicable Article 23 or Article 24 EUCC.
88. Where the authorisation is withdrawn, the CB or ITSEF should stop the promotion of the authorisation of their entity from the moment of the withdrawal decision.
89. In the case there are successors for the evaluation and certification activities, the compliance responsibilities of the initially authorised CB or ITSEF should be transferred to the successor which is authorised. Where the successor is performing evaluation and/or certification activities under assurance level ‘‘high’ and takes over the activities of the CB or ITSEF for which authorisation is withdrawn, it is presumed to be the successor-in-interest the moment it obtains its authorisation decision from the NCCA.
90. Where the CB or ITSEF is subject to running investigations, complaint procedure or legal procedures, the NCCA should provide a decision related to suspension or restriction, depending on the case-by-case situation, until a final verdict has been established.

12 COMPLAINT HANDLING

91. The monitoring and supervising NCCA is in accordance with Article 58 (7) (f) responsible for the handling of complaints when it comes to certification under assurance level ‘high’. As the NCCA is the responsible body for the authorisation procedure, it also needs to use the complaints procedure for the CB, the ITSEF and their customers or any other third party with a related interest which may have concerns or complaints related to the authorisation of a conformity assessment body and its procedure. They have the right to be heard, to be informed on their status of their complaint and need to be informed by the NCCA of their right to an effective judicial remedy in accordance with Article 64 CSA. The NCCA needs to make the complaints procedure online available and it should be easy to access the related information on the procedure and to find the information to file a complaint.

13 PENALTIES

92. Authorisation is an element of the EUCC therefore Article 65 CSA should apply to authorisation requirements.

14 ANNEX I: INFORMATION TO BE PROVIDED BY THE NCCA

The NCCA should see to it that the application information can be obtained digitally in the language of its Member State and in English[29] and should provide at least:

1. An application form;
2. Information related to the specific application procedure, including information on the recommended and necessary preparations for ITSEFs and CBs[30];
3. The list of ICT product categories and protection profiles to which the authorisation extends;
4. The overview of the necessary documentation that should be provided to start the application procedure, which should include at least:
   a) The formal statement of accreditation issued by the NAB[31], or if not available yet a statement of the NAB that they are in the process of handling the application, or are in process of accreditation[32];
   b) The documentation to be provided by the ITSEF related to paragraph 6.2.1 point 42 and for the CB the documentation to be provided under paragraph 6.2.2. point 45;
   c) The documentation demonstrating the competence management system that includes the:
      - Required technical competences for the testing and related evaluation activities performed by the ITSEF in accordance with Article 22 EUCC[33] and specified under Annex II, taking into account chapter 4 point 35 and 36;
      - Required technical competences for the CB activities performed in accordance with Article 21 EUCC and specified under paragraph 6.2.2 point 48 and 49, taking into account chapter 5, point 35 and 36;
      - Required competences for the technical and organisational measures (TOMs) for the CB and ITSEF to effectively protect confidential and sensitive information specifically addressing the risks related to their activities performed under assurance level ‘high’ in accordance with chapter 10, paragraph 10.1.
   d) The documentation demonstrating the compliance with the required TOMs for the CB and the ITSEF in accordance with chapter 10, paragraph 10.2;
   e) The information related to the authorisation report of the ITSEF in accordance with Annex III;
   f) For the authorisation of the CB: the documentation demonstrating that the CB is collaborating with an authorised ITSEF. This should include amongst others:
      - A proof of contract addressing the exchange of information and the conditions that apply;
      - The means and aspects/fields of cooperation;
      - The procedure for re-use of evidence in line with chapter 4, point 19 coming from another CAB and how this information is exchanged and under what conditions;
      - The right of the CB to request information and visit the ITSEF for the purpose of the certification decision, and;
      - The elements of cooperation related to the monitoring of compliance of the certified product (e.g. the request by the CB to the ITSEF for the support in a sampling procedure, or vulnerability handling procedure);

[29] To allow CBs and ITSEFs to be authorised in other Member States, information should be made available in English as well.

[30] This includes the necessary guidance for ITSEFS and CBs that have no previous experience under SOG-IS MRA.

[31] For accreditation of the CB the SoA ”Accreditation of the certification body” applies. For accreditation of the ITSEF, the SoA “Accreditation of ITSEFs for the EUCC” applies. Both documents are listed under Annex I point 2 EUCC.

[32] Note that a formal statement of accreditation by the NAB is a prerequisite for obtaining authorisation decision

[33] The ITSEF and the CB need to be able to demonstrate the technical competences related to the scope of the Authorisation which needs to be indicated in the application form. Based on the scope definition, the applicable State-of-the-Art documentation listed in Annex I Commission Implementing Regulation (EU) 2024/482 identifies the technical competences that will be subject to authorisation.

g) Where the CB and/or ITSEF is/are already authorised for another scope, the provision of evidence related to the existing authorisation and the applicable authorisation report[34];

5. The description of the authorisation procedure: the steps and indication of the content, the overall planning of the entire procedure, the estimated timelines and information related to the complaint handling. In the case where, based upon the scope of authorisation besides the structured interviews other methods of assessments are part of the authorisation procedure, they should be made public by the NCCA. Other methods of assessment to demonstrate compliance as described under chapter 4, paragraph 4.1.1 point 22 (c);
6. In the case of a first application of authorisation under EUCC, the information that should be provided to review of at least one pilot certification procedure[35] (including a plan for evaluation & certification) and information regarding the re-use of evidence for the pilot certification which may be provided in accordance with EUCC;
7. Where additional requirements to the pilot certification apply, the specification of these additional requirements defined by the NCCA, which may be:
   a) Additional demonstration of certain selected testing or related evaluating activities or certification activities to support the demonstration of the specific competences,
   b) The performance of a specific review of a testing or related evaluation or certification activity, or;
   c) The performance of a specific use case in the field of expertise, or;
   d) The participation in a defined challenge/simulation exercise for conformity assessment bodies.
8. Where the application is related to the renewal of authorisation, the NCCA should provide and make digitally available:
   a) The appropriate application template for renewal of authorisation;
   b) What (elements of or only updated) documentation under what rules and conditions should be provided in the case of renewal and what the conditions for re-use of evidence are (see chapter 4, point 19).
   c) The recommended time indication for filing the application for renewal before expiry of the authorisation, being 6 months;
   d) The description of the renewal procedure (the steps that need to be taken taking into account that no pilot certification is required);
9. The description of the compliance audit procedure by the NCCA and the necessary information to be provided;
10. The description of, or reference to the notification procedure and related communication to the authorised conformity assessment body and the description of the procedure related to any changes related to the CB and ITSEF that impact the authorisation requirements leading to renewal, restriction or temporary suspension, as described under chapter 8, paragraph 8.1, point 70.

[34] When the ITSEF has been authorised by the NCCA, the report should have a unique number and should be registered by the NCCA.

[35] See Article 21 (2) and Article 22 92) EUCC.

15 ANNEX II: THE ITSEF TECHNICAL COMPETENCES TO BE ASSESSED

The ITSEF should provide the documentation demonstrating that the ITSEF ensures that it has all the necessary technical competences and is able to maintain the up-to-date technical competences in at least the following areas:

1) The ability, knowledge & skills to design, to use up-to-date threat intelligence and is able to analyse the risks and perform and assess the related risk assessments, understand and is able to translate this information to up-to-date evaluation methodologies appropriate for the scope of authorisation;

2) The ability, knowledge & skills to design, to detect, analyse and perform testing/evaluation methodologies developed for assurance level 'high' that are taking into account a risk-based approach, related to the scope of their foreseen application to authorisation, and which are used for testing the resilience against state-of-the-art cyberattacks performed by skilled attackers with significant skills and resources. This implies the ability, knowledge and skills to apply a comprehensive and well-structured set of procedures and flaw hypothesis methodology (whereby specifications and development and guidance evidence are analysed and then potential vulnerabilities in the TOE are hypothesized, or speculated), as required by ISO/IEC 18045 for the evaluation of different types of products or technologies and the use of the applicable guidance to support the evaluators;

3) The ability, knowledge & skills to translate of these types of cyberattacks into the different evaluation methodologies in terms of design & re-design, selection, operation and evaluation and optimisation of the applied methodologies, as there is not a unique way to perform an attack and it may be possible to spot the same vulnerability using source code analysis, fuzz testing and manually devise this, or other testing methodologies;

4) The ability, knowledge & skills to design/develop, perform and evaluate attack potential calculations using the applicable table provided by ISO /IEC 18045[36]; for the applicable Technical Domain of Hardware devices with security boxes we refer to the SoA: "*Application of Attack Potential to hardware devices with security boxes"* of Annex I (1) (b) (3) EUCC; for the applicable technical Domain of Smartcards and similar devices we refer to the SoA: *"Application of Attack Potential to Smart cards"* of Annex I (1) (a) (7) EUCC;

5) The ability, knowledge & skills to have a thorough understanding of the capabilities and limitations of available tools selected, justified and used under assurance level 'high' (automated vs the manual use requiring more time and expertise; and the understanding and expertise to use development tools, analysis and attack tools (e.g. source code analysis and coverage tools, test benches for invasive and semi-invasive techniques, side channel analysis, perturbation, tools for physical tempering, etc.) and IT systems necessary for the evaluation activities under assurance level 'high', the ability to where necessary to be able to find 'work arounds' for adequately testing the ICT product that allow to analyse and determine the level of resistance of the ICT product or protection profile;

6) The ability, knowledge & skills to describe the evaluation activities and the findings in a technical sound, consistent and verifiable, logical and structured order, despite the complexity of the evaluation activities under assurance level 'high' they should be easy to follow for outsiders of the evaluation;

[36] For AVA_VAN level 3 this requires the ToE to be resistant to 'Enhanced-Basic' attacks

7) The ability, skills and knowledge of cryptographic algorithms, protocols, and relevant expertise in cryptographic evaluations, and capability to check for the presence of well-known vulnerabilities in cryptographic protocols;

8) The ability, skills and knowledge or each technology type or in the area of work of the evaluator, knowledge of the product type in scope of the authorisation, including:

   I. typical feature set, use cases, and operational environment;

   II. architectural concepts, design and implementation methods and relevant implementation languages and tools;

   III. associated development and production processes;

   IV. known vulnerabilities;

   V. CAPEC™ applicable attack patterns[37];

   VI. Relevant attack methods already used in Common Criteria evaluations, especially based on the EUCC technical domains that may be relevant for the product type.

9) The ability, skills and knowledge to select, justify and apply the proper source code analysis techniques, to select justify and use in the laboratory environment or where necessary, the production environment, the different types of penetration testing (Black-box, Grey-box and Chrystal-box or White-box), selection, justification and use of penetration testing tools and debugging tools;

10) The ability, skills and knowledge to select, justify and use open source tools (e.g. gdb, ollydbg, wireshark, nmap, metasploit framework, scapy, etc) tools for adaptation of opensource software developed by the evaluator (e.g. IDA Pro, Cryptosense Analyzer, a commercial fuzzer, etc.) and AI based tools for software testing allowing to identify attack paths or to exploit vulnerabilities and hardware attack tools (e.g. portable oscilloscopes, logic analyzers, USB microscopes, special screwdrivers, soldering/desoldering/ rework stations, memory programmers, low-end glitching stations);

11) The ability, skills and knowledge to perform enhanced-basic and more complex reverse engineering;

12) The ability, skills and knowledge to monitor the ICT product evaluations or protection profile evaluations, where applicable for the technical domains;

13) The ability, knowledge & skills to process the Evaluation Technical Report in accordance with Article 10 (4) EUCC including the capability to write, and use correct English;

14) The ability, knowledge & skills to develop procedures for the administrative handling, the maintenance and retention of all documentation in accordance with the quality management;

[37] CAPEC™ stands for the "Common Attack Pattern Enumerations and Classifications" It helps by providing a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. It can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses. Source: CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™) (mitre.org)

15) The ability, knowledge & skills to technically support the CB in the vulnerability handling procedure by analysing the impact assessments, to perform upon the request of the CB technical evaluation checks to verify the remediating measures that need to cover the vulnerability;

16) The ability, knowledge and skills to effectively protect sensitive and confidential information by means of implementing and maintaining TOMs, as well as to exchange this type of information with their CB, customer, and with the NCCA (see Chapter 9, Information protection);

17) Where the scope of authorisation is related to a specific technical domain or a specific protection profile describing specific evaluation methods, the specific technical competences in indicated in the applicable state-of the-art document listed under Annex I Commission Implementing Regulation (EU) 2024/482 should be demonstrated as well.

16 ANNEX III: THE CONTENT OF THE AUTHORISATION REPORT

The authorisation report should include at least the following elements, information and applicable findings:

a) The address, name and logo of the NCCA, the URL of the website, their logo;

b) The unique registration number in accordance with point 62 and date of registration of the authorisation report and the unique accreditation number provided by the National Accreditation Body. Where the authorisation concerns a renewal, a reference to the previous report (including the name of the report and date of authorisation, unique registration number and its validity) should be provided;

c) The entity name, address, country and contact data (including but not limited to: the responsible contact data and name of the contact person responsible for authorisation in the CB and/or ITSEF, the URL of the website);

d) The registration data of the legal entity and the name and contact data of the legal representative of the CB or ITSEF (this should be natural person);

e) The description of the scope of the authorisation: the category(ies) of ICT products and or protection profiles for which the authorisation applies and their applicable assurance level specifications (e.g., AVA-VAN level, technical domain);

f) The date of registration of the application and application number;

g) A description of the NCCA authorisation team and their functions/roles in accordance with paragraph 6.1 point 41;

h) The description of each of the authorisation assessment activities related to Articles 21 (1) and 22 (1) of EUCC: It should include what is assessed and by what means[38];

i) The assessment activities should include the date of performance, the assessed departments (in the case of general delegation or prior approval in accordance with Article 56 (6) CSA the report should describe for each of the assessment activities which CB entity and department was subject to the assessment of the activity), the location of the assessment[39], and for each of the assessment activities the names and roles/functions of the NCCA authorisation team members that performed the assessment activity, the names of staff and roles/functions of the CB/ITSEF staff that participated in these assessments;

j) The references to the applicable evidence including where applicable and specify the re-used evidence and the related source. This may include in case of renewal - elements of - the previous authorisation report. The date of the initial evidence and the justification for re-use should be provided. Each evidence reference used in the assessment should be registered and have a specific number. These numbers can then should be referenced in the description of the assessment activity. The report should contain an annex where the evidence description and the evidence numbers are provided;

k) Where during the assessment additional assessment activities (described under paragraph 6.2.3) are performed, this should be included in the description of the assessment activities, indicating by whom they were performed of the NCCA authorisation team, and roles/functions

[38] The 'means' comprise amongst others of the structured interviews and their purpose, document reviews; other assessment activities like demonstrations, evaluation and certification assessment tools testing & material and test bench assessments; audits; site visits; certification review-, validation- and decision procedures.

[39] Where the assessment activity is comprised of document review, this can be the location of the NCCA.

of the CB/ITSEF staff that participated in these additional assessments with the inclusion of reason and purpose of the additional activity and provision of the dates of these assessment requests made, and when they were performed;

l) The findings should be described for each of the assessment activities and scored by indicating the following indications: ‘compliant’, ‘minor/major non-conformity’, ‘minor/major non-compliance’;

m) Where applicable, the description of the finding should be complemented by a description of the required fixes that the NCCA requested upon point 1 (l). The indicated timelines for correction and the indications of the NCCA authorisation team should be provided with the dates that these fixes were provided to the NCCA authorisation team and proof and date that they were approved;

n) The draft report should be subject to NCCA internal but independent review and signed for internal control by the coordinator of the authorisation team before the draft report is send out to allow the CB or ITSEF to provide their comments on the draft report. Where the CB or ITSEF have comments upon the draft, these comments should be included in the section of the findings as an additional element;

o) The conclusions and verdict indicating ‘authorised’ or ‘failed authorisation’ of the authorisation should be included and in the case of verdict “authorised”, the duration and date of the validity and a section including the possibility to start a complaints procedure including a link to the procedure should be provided;

p) The executive summary;

q) The (digital or ‘wet’ signature) signature of the legal representative of the NCCA;

r) Annex with the list of used evidence numbers used in the report. In the case of renewal of authorisation, the references to the evidence used in the previous report should be provided, including the evidence numbers.

17 ANNEX IV: THE TECHNICAL & ORGANISATIONAL MEASURES (TOMs)

The CB and ITSEF should have the following policies and procedures in place that are implemented, trained and maintained and which should apply to the entire CB and ITSEF, including where applicable all subsidiaries and establishments in the EU:

1) Risk assessment and risk analysis;
2) Business continuity, such as backup management and disaster recovery, and crisis management;
3) Incident handling including reporting to the NCCA and CSIRT which should follow:
    a) for the reporting of incidents to the CSIRT the reporting by the CB and ITSEF as entities the procedure in analogy to Article 23 NIS2 should apply;
4) Supply chain security, including security-related aspects concerning the relationships and transfers of data between each entity and of its direct suppliers or service providers taking into account the following:
    a) the vulnerabilities specific to each direct supplier and service provider;
    b) the overall quality of their services and cybersecurity practices of their suppliers and service providers, including their secure development and lifecycle procedures.
5) Security in network and information systems including their acquisition, development and maintenance, including vulnerability handling and a coordinated vulnerability disclosure policy. It is advisable to review international standards like the ISO/IEC 2700x series or national standards for suitable content. These systems should be appropriately documented;
6) Cryptography policy and effective encryption mechanisms including the appropriate use of encryption to store sensitive data at rest (e.g.: hard disk encryption) and in transit (i.e. outside the control of the CAB, e.g. for e-mail, voice/video or physical media transported outside the CAB). Choice and strength of algorithms should be based on risk situation and the state of cryptography (e.g.: length of keys, use of quantum-safe algorithms).
7) Human resources security, commensurate to the estimated attackers for tangible evaluation and certification assets. This focuses on preventive measures and should include reactive measures in case of incidents as well, which is entailing amongst others:
    a) Non-CB and non-ITSEF personnel with temporary access to assets of the CB and ITSEF (e.g.: visitors, external functions or companies) ensuring that their access is limited as much as possible and supervised;
    b) Overall access policy to assets of the CB and ITSEF for CB and ITSEF personnel, based on the need-to-know and need-to-be principles and including an authentication policy consisting of multi-factor authentication. Additionally, the CB and ITSEF should operate a policy for secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate. This implies logical access rules commensurate to the risk of the individual devices (i.e.: network context, attack surface) using multi-factor authentication where technically possible and requiring sufficient strong mechanisms (e.g.: length of passwords);
    c) A staff integrity screening policy for those persons that have access upon the need-to know-and need-to-be principles to confidential and sensitive information obliging to perform an integrity screening on a regular basis;
    d) Basic cyber hygiene practices and cybersecurity training;
    e) A policy related to work ethics with special attention for:

I. Fraud prevention;

II. Prevention of inside intruder incidents leading to leaking of information by: espionage, or deliberate publication of confidential information;

III. Neglect of duty to meet cybersecurity requirements;

IV. Encouragement of reporting personal security incidents and use of these cases for cybersecurity awareness (training) programs;

8) Physical security;

9) Asset management including reduced network connectivity for devices used in the context of the CB and ITSEF to limit the attack surface, e.g.: dedicated networks for CB and ITSEF activities; Trustworthy software installation and maintenance (upgrade) procedures including measures to limit access of 3rd parties on CB and ITSEF assets during installation/upgrade;

10) Safe and secure destruction policy of media;

11) Where artificial intelligence (AI) is used for conformity assessment activities, the ITSEF and CAB TOMs to handle AI specific risks, e.g., accuracy or robustness;

12) For the Specific TOMs that apply for the ITSEF and the developer during evaluation of ICT products, the SoA related to 'Minimum Site Security Requirements, version 1.1' as annexed to EUCC under annex I (a) (2) should apply.

18 ANNEX V: THE COMPETENCE OVERVIEW TO BE PROVIDED BY THE CB AND THE ITSEF

In this annex, a recommended template is provided for the conformity assessment body to provide to the NCCA for assessment of the required competences related to authorisation.

The conformity assessment body should have and provide an overview of the competence management system for all staff (internal and external).

Key critical functions within the conformity assessment body (CB or ITSEF) are functions that are key to perform the conformity assessment activity, without the function, the activity cannot be performed by the conformity assessment body. For the key critical functions, the conformity assessment body should have a policy in place that ensures continuity of the conformity assessment activity. The policy should include the following aspects:

- The strategy and long-term continuity of the key critical functions (describing the relation to business plan and KPI's of the conformity assessment body)
- The identification of the key critical functions and required competences
- The fulfilment of the key critical functions (% internal, % external staff)
- The succession planning related to key critical functions (taking into account where applicable external staff and related dependencies)
- The learning & development policy and planning (taking into account where applicable external staff and related dependencies)

Department & conformity assessment activity description	Related job description	Staff member (pseudonymization) and indication internal or external	Required competence	Scored competence

General competence management elements recommended for assurance level 'high' context are:

- The elements of competence, competency levels and the measurement of the elements of competence are drawn from 19896-1 and if they differ, they should be commensurate with the objectives and equivalence should be demonstrated;
- The knowledge, skills, experience and education, and the requirements from ISO/IEC 19896, and if they differ, they should be commensurate with the objectives and equivalence should be demonstrated. Where ISO/IEC 19896 misses requirements for a certain function within the CAB, analogous or equivalent requirements should be used instead;

- For the high assurance level, there is no common baseline of evaluator's competence requirements for different technologies and technical domains (e.g. mobility, network devices, etc.), but each ITSEF should define and handle its own set of requirements based upon the authorisation scope. The types of technology used to structure and specific knowledge are described and skills requirements for the certifiers are defined or refined by the CB according to the type of products they certify, and their underlying technologies;
- The knowledge required for reviewing security assurance requirement classes evaluation reports are specified based on Annex B of ISO/IEC 19896-3 ITSEF staff (evaluators) capable of conducting AVA_VAN.3 evaluation activities should meet the competence requirements described in [19896] for the relevant SARs (AVA_VAN.3, ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1 and ATE_DPT.1, etc.);
- The knowledge recommended for reviewing security functional requirement classes evaluation reports are specified based on ISO/IEC 19896-3.

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu